

1) 'Did you have any particular motivation for the hack or specific things you were trying to grab?'

Not really. It was a once in a lifetime situation, just finding the right things at the right time. I will be more specific when I answer the question of how we got in. Saying too much more than that would give up too much information about us, unfortunately.

2) 'Is there anything you found that you were especially excited to get?'

We were really excited to find data for the currently in-development games. Of course it was a given, being that we had basically full access, but it was still surprising to find, even if it would've happened anyway.

3) 'Were you surprised by anything that was unearthed? I remember at first you didn't think there was any pre-gen4 stuff until people went digging through the Box dump.'

I was surprised by how skilled individuals were able to do a deep dive into some of the data - getting the builds to work, the recent source code that was missing parts, etc. When we said there wasn't any pre-gen4 stuff, we meant there wasn't any builds or source code.

4) 'What do you think of the community reaction to the leaks?'

Well, the community reaction is normal. There is a large mix of people doing a good job, people creating drama, people shitposting, people on 4chan being morons - "WE WANT EVERYTHING, BUT WE DON'T WANT TO TAKE ANY RISK, AND WON'T DO ANYTHING OURSELVES. FUCK YOU LEAKER, DUMBASS!". It was fun to see, and especially all the theories of what and who we are.

5) 'You've been really active in the community, what made you stick around and keep talking to people unlike typical leakers?'

In reality, being "around" could be considered an opsec failure of some sort, but it only becomes one when it's over a long period of time.

The plan was to disappear after, at most, 30 days, no matter what. Everything that we say is carefully chosen and reviewed, and we did our best to leave a false trail in many of our messages to give potential false hints to who we are, where we are, etc.

We did kill all our accounts at the end of the first leak wave, but we kept our promise and posted ZA at the right time.

6) 'Can you clear up the rumor that you took employee personal information?'

We cleared this up a while ago, but let's do it again: We did NOT publish any personal information, excluding very few documents found within the data that are limited to information such as names and corporate emails, which were already public information. Also, there was no "ransomware-like" action in all of that, we never talked to GF, never asked for a money payout as ransom, never asked them for anything.

This rumor comes from the announcement made by GameFreak on their website on October 10th, two days before we started releasing the data.

While we admit it does seem pretty suspicious that we would start leaking data right after the announcement, it was actually completely by coincidence, and we were not made aware of the press release until afterwards.

The press release refers to "Names, Surnames, and Corporate Emails" as part of the "leaked" data. They had to assume that their Active Directory was stolen, as we did download a backup of one of their AD virtual machines as a VHDX drive image.

We did this, because we needed to get accounts and hashes to crack in order to elevate our access. Despite having access to an account with domain admin, certain portions of their IT were still limited (their Confluence, Perforce, and the access we had within the CLI.) So, even if we did take a copy of the Active Directory which included that information, it wasn't with the intention of taking personal information relating to employees, and it barely contained any information anyways.

7) 'What prompted you to start releasing stuff? Were you always planning to or was it only because they noticed?'

Like we said before, there wasn't any reason in particular to start at this moment. It was just good timing more than

anything else. We were always planning to release the data, from the very first day we gained our access inside GameFreak's systems.

8) 'As much as you're willing to reveal, how did you get into GF and what led you up to it?'

We were able to gain access to a random Japanese contracting company that GameFreak had outsourced to. We got in by complete chance, and we only got this access by complete luck in looking for videogame related data.

At some point, we noticed they were working with GameFreak, and that they had whitelist access to a few IPs, including GameFreak's Confluence and GitLab.

We were able to find an account belonging to the contracting company that had access to the GameFreak GitLab, and had access to only a single repository from an old, non-pokemon related project. After having a look around at everything we could access, we noticed we were completely locked down, and couldn't do anything. So, we started to look at more obvious and less discrete ways to elevate our privileges inside GameFreak.

We were able to create repositories using the account we had access to, under our username (/username/repositoryname/) and we noticed that their Gitlab had the CI/CD feature enabled, and that we had access to a few

we could select and use, and they were not configured to have any restriction to any specific user group or project, so anything could be run on them.

From here, we created a CI/CD command file, and ran a command that dumps the environment over text, base64 format, to bypass Gitlab's automatic secret removal from CI/CD logs, and print out on STDOUT.

In there was an account named CI_ADMIN and the accompanying password. "No way, really?" we immediately thought. We tried it on GitLab itself (as Gitlab was configured to have a LDAP login, so employees can use their regular GameFreak AD account to log in), and it worked. It connected us to the main "root" account of their Gitlab, the superadministrator account with the highest privileges. This was probably the dumbest way we have ever managed to get admin access to something as sensitive as Gitlab. With this account, we had windows local administrator permission on some runners and were able to read contents from a few user Desktop folders on those runners. For some (stupid) reason, one of them ended up having a copy of a "gitlab.rb" file. Yes, it was the Gitlab server config file, and yes, it did have a new AD account in it for us, inside the LDAP binding configuration (that allows Gitlab to connect to the LDAP Active Directory). Yes, the account was the "GF_BIND" account we already talked about in the past, which was a domain admin. Well. We were a domain admin. We had access to anything we wanted, minus a few things where domain admin permissions were not linked to the equivalent local permissions, like in Confluence, Perforce, Gitlab (but we already had admin access to Gitlab anyway.)

Beyond that, there isn't a lot more left to tell. We took time to look inside the GameFreak network, looking inside their Windows servers, SMB shares, etc, until we were noticed and kicked out. We don't know exactly how they managed to catch us, but it may be because they noticed a spike of activity on their SVN server that we were working on taking (this is why XY's source was incomplete) • The first thing they did was revoking access to the firewall whitelist (either for everyone a whole network shutdown, or just for the company we were entering from). We kept access to their BOX enterprise environment for a few days (from a few API keys, all accounts were locked), so we tried to download as much data as we could, but we didn't have a setup allowing quick and large exfiltration, so we were not able to get as much as we would have liked to. We did have to create some scripts to work our way in, allowing us to communicate with the BOX api safely (and their API is awfully documented), and being able to navigate through SMB and executing commands through SSH on computers from their network - all of this was done in a non-interactive CLI that runs commands from a defined list, since it runs from the Gitlab CI tasks we ran. Getting a working SSH command over a script that runs on Windows that was started from a CI/CD running job was definitely not the easiest thing we've had to do.

9) 'How long did you have access for?'

Without giving up too much information, we had access between two and four weeks, around August 2024. As stated previously, we were noticed and kicked after Pokemon Worlds.

10) 'Is there anything else you want people to know?'

We already stated this fact, but we want to say it again: We don't care about building fame, getting money, whatever. We will disappear anyways, we are not coming back, we are just keeping our words and posting what should be. Why

would any of that matter?

Moral related questions are more difficult to answer, because, after all, we did hack GameFreak. That is already not really a

morally acceptable thing from a moral and ethics point of view. However, that doesn't stop us from caring about some aspects of it, and keeping private what should be kept private. It's not the most fun to keep things private, but it must be done. If anyone is not happy with that or doesn't believe us, then have fun, and go do the same things and take all the same risks that we took. (Don't. You'll go to jail.)

11) 'What was the reason we weren't able to get stuff like documents and pokemon/character concept art for gen 8+?'

Most of the information for S/M Us/Um were... nowhere to be found. We luckily found a copy of the git repository archive in a random folder from their Box env (copy that was more recent than the already leaked one from the gigaleak), a few builds elsewhere, but that's all. We think it might be a huge luck-based reason that we were able to access such a huge data stash for XY (which still had dedicated windows network share for it!). We think they were really having IT difficulties back in the 3DS era, and changed how their systems work a lot. They were also spawning an internal wiki for each new game, each time a new one with a new system and new url, we were lucky to find a random backup of the sango wiki. Also, the 2018 hack may have indirectly forced GF to clean some of their old IT systems and discord those old wiki/old file share servers. For switch based games, most of the data was on Confluence. We stated that before, but unfortunately, the confluence export module was not working correctly and we couldn't download exports for spaces if it was more than 1GB. That's why we were not able to get many files for all of the switch-era games.

12) 'Are you a hardcore Pokemon fan yourself? If so, how did you look at the content you found from the perspective of a fan'

Yes we are, we would not talk about a "once-in-a-lifetime occasion" if we were not ;) We took a long look and had lot of fun compiling most of the old stuff (especially the DS-era part), we were sad to not find much more info about the HGSS pokewalker, but in the end we were very happy because we precisely found data right at the point where the gigaleak stopped. We literally found data starting from Platinum and all game afters but not before (except for some documents and graphics found on Box), and we find that pretty funny as it's literally where the gigaleak stopped in terms of pokemon data.

13) 'Was there anything you wish you could've gotten that was simply not an option or was not able to happen due to constraints?'

More build, especially of the others switch games. And we were really really deceived to not find a copy of the BDSP source code as it was stored inside ilca's own gitlab. We tried to pivot from gamefreak to ilca but we were unable to do it due to the heavy network restriction in GF network. we would have loved to be able to better dump the gitlab, as we know we missed a few relatively important repositories. But the community did a great job and managed to make relatively everything work despite those missing bits.